

Web-Conferencing Using Zoom - Best Practices and Settings for Increased Security

Web-conferencing with Zoom can be a powerful tool. Users/hosts should follow best practices in order to best secure conversations with all participants. Zoom.us has increased security recently with different features and default settings designed to minimize security lapses that occurred after a recent dramatic increase in public use. The following are some examples of best practices and security settings to consider when web-conferencing to significantly increase security during your sessions.

***Please NOTE** - It is positive practice to have parent/guardian permission before Zooming with students. Recognize that video conferencing is potentially much more intrusive to a home than a regular phone call, as there is an increased likelihood of overhearing background conversations or viewing background activities happening in the home. Permission from the parent ensures that guardians are aware a video conference is taking place and provides the opportunity to manage the conference environment or decline participation.

Hosts have the ability to set and adjust the available features and settings to fit the specific needs of each Zoom session. Consider each Zoom session separately, and only enable features that are needed and will provide the level of security appropriate for each situation.

To Access Settings

1. After signing into your Zoom account, click on the Settings link on the left hand side of the screen.
2. Scroll to see a list of all advanced setting options.
3. When modifying settings
 - a. Pay attention to the toggle switch. Blue is ON and grey is OFF.
 - b. Some features use selection bubbles instead of toggle switches. A dot in the bubble is ON and an empty bubble is OFF.
 - c. A few setting changes require the additional step of clicking a SAVE button when changes are made. Be sure to click SAVE if a button is available.

To Access Dashboard Options

1. After signing in to a LIVE Zoom session, note the multiple areas that dashboard options may appear.
2. Most options appear on a toolbar at the bottom, right, or top of the screen.*Note that positions of toolbars and options may change when in full screen mode or if a host is sharing a screen.

Safety Settings to Prevent Unwanted Participants

The best way to manage security is to prevent security issues from occurring at all. There are several security settings that can be useful to eliminate the opportunity for unwanted/unexpected people to enter your session. Use these whenever possible and appropriate for adult sessions and always with student sessions.

Require Password for Manual Entry- This is automatic and should not be removed. (In Settings)

1. A password is **automatically** generated for each meeting by default.
2. NOTE: Participants entering a meeting through a link provided from the host DO NOT need/use the password. It is only for those manually entering the Zoom session ID to access a meeting.

Require a password for Personal Meeting ID (PMI) 

☐ Only meetings with Join Before Host enabled

☒ All meetings using PMI

Password 715028 

How this feature increases security:
Zoom.us made the password automatic as an additional measure to limit unwanted guests in a session.

Some unwanted participants were entering Zoom sessions by using computer programs to 'guess' active session IDs. Requiring a password in addition to the session ID minimizes/eliminates that issue.

Most hosts provide wanted participants with direct links to a session, usually through an email or by posting it in a secure location such as a Google Classroom. Participants clicking on a direct link provided by a host will not need to use the password and will not even be aware that the password exists.

Use the 'Waiting Room Feature' (In Settings)

1. This is turned **ON** by default.

Waiting room 

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled. 

How this feature increases security:

The waiting room feature is ON by default as one way Zoom.us attempts to

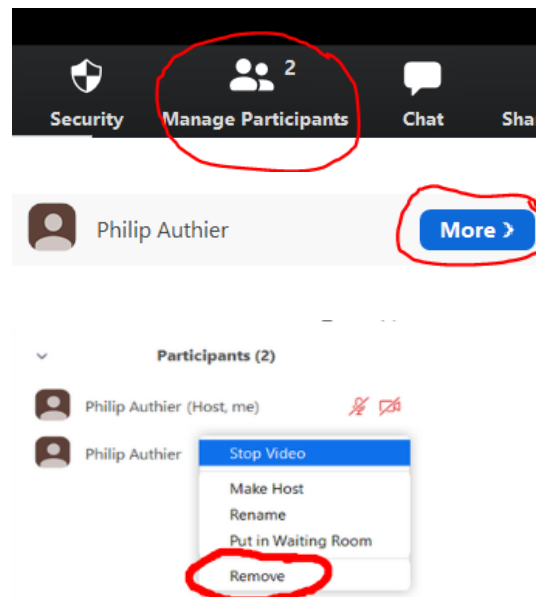
2. Do not turn it off when conferencing with students. 3. Consider leaving it ON even when conferencing with adults. 4. Participants joining the zoom session are not immediately admitted, and see a message alerting them that they must wait to be admitted by the host. 5. A host can view names of all participants in the waiting area and admit ALL or one at a time.		keep unwanted visitors from joining a session. This is another layer of protection to prevent unwanted participants from unexpectedly joining a session. In most situations, a host knows the identity of wanted participants and can easily identify an unknown name in the waiting room. In most situations, a host should not admit uninvited or unknown participants. *See below for related information on name changes.
TURN OFF 'Allow participants to rename themselves' feature (In Settings) 1. This feature is ON by default. 2. Set this feature to OFF. 3. *NOTE - This can be turned OFF or ON during a live session by clicking the Security Shield icon.	Allow participants to rename themselves Allow meeting participants and webinar panelists to rename themselves.  	How this feature increases security: When set to OFF, participants will be forced to use the name attached to their email addresses before can they join a meeting. If set to ON, participants have the ability to enter alternative names. Preventing the choice of alternative names increases a host's ability to know and control who is joining a session.

How to Remove Unwanted or Unruly Participants

In the unlikely event that an unwanted participant joins a session, hosts should know how to quickly and permanently remove them. When Zooming with students, there may be situations where it becomes necessary to temporarily remove an unruly or distracting participant.

Permanently Removing a Participant from a Session (On Session Dashboard)

1. The host can remove **any** participant from a session.
2. Click “**Manage Participants**” on the bottom of the screen.
3. Place your mouse over the participant’s name and click **More**.
4. Click **Remove** (can only be done one participant at a time).
5. Once a host removes a participant, the participant cannot rejoin the session.
6. If a host wants to temporarily remove a known participant, select **Put in Waiting Room** instead of Remove.



How this feature increases security:

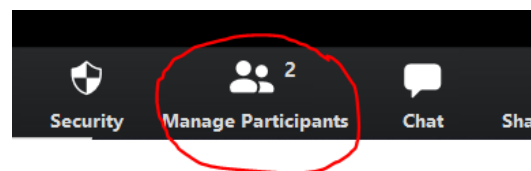
A host can remove any participant from a session. All hosts should know how to do this **quickly**, in the event it is necessary to remove an offensive participant.

This may be necessary if an unknown/unwanted participant joins your session.

*NOTE - Should a host accidentally remove a known participant and then want to allow that participant to return, a host can temporarily change a Zoom settings for a session to Allow Removed Participants to Rejoin, but that option is OFF by default.

Temporarily Removing a Known Participant from a Session (On Session Dashboard)

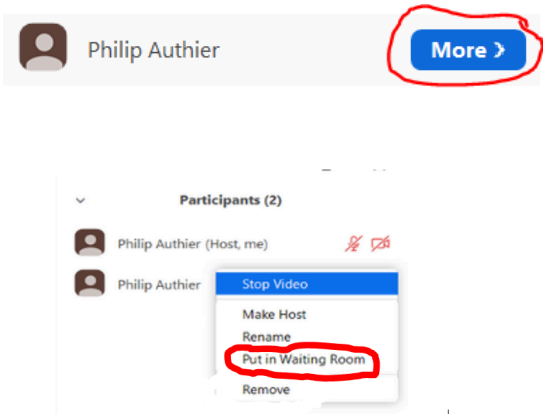
7. The host can remove **any** participant from a session.
8. Click “**Manage Participants**” on



How this feature increases security:

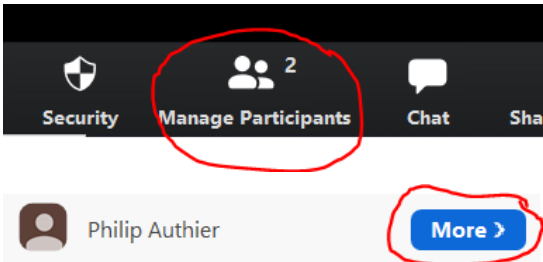
There may be situations where a host may need to temporarily remove a known participant from a session.

An example of when this might be useful

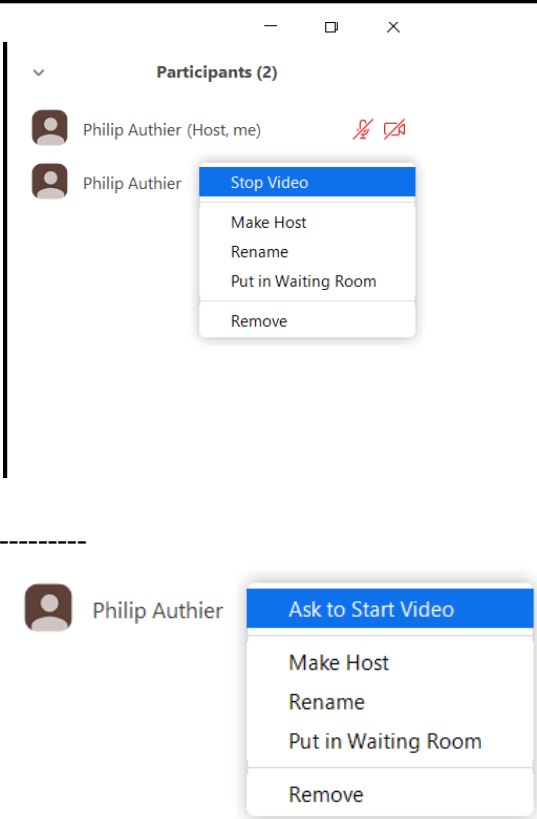
the bottom of the screen. - Place your mouse over the participant's name and click More. - Click Put in Waiting Room (can only be done one participant at a time). - The host can then choose if/when to admit the participant back to the session.		would be temporarily removing a student that is being uncooperative, unruly or distracting. *NOTE - This might also be useful if accidental but potentially embarrassing activity takes place during the session in a participant's home or location.
---	--	---

Using Settings and Features for Managing Participant Video and Audio

When Zooming with large groups of participants or with students, it can sometimes be difficult to manage. Zoom has several settings and features that can be used to help facilitate Zoom sessions.

Turning OFF a Participant's Video (On Session Dashboard) - The host can turn off video for any participant. - Click "Manage Participants" on the bottom of the screen. - Place your mouse over the participant's name and click More. - Click Stop Video (can only be done one participant at a time). - Once a host stops the video for a participant, the participant will not		How this feature increases security: A host can turn off video for any participant. Know how to do this quickly, in the event it is necessary to stop a participant's video. This may be necessary if there is distracting activity, purposeful inappropriate activity OR if accidental but potentially embarrassing activity takes place during the call.
--	---	---

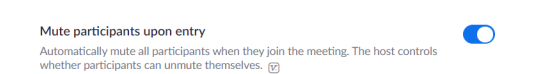
be able to restart unless the HOST gives access by clicking “Ask to Start Video” by the participant’s name.



Setting ALL Participants’ Audio to MUTE when entering a session (In Settings)

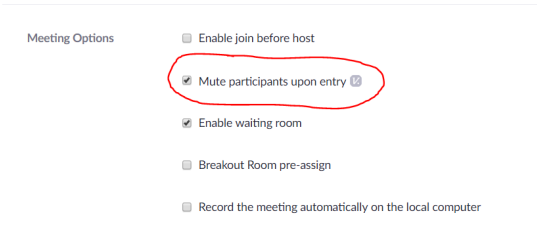
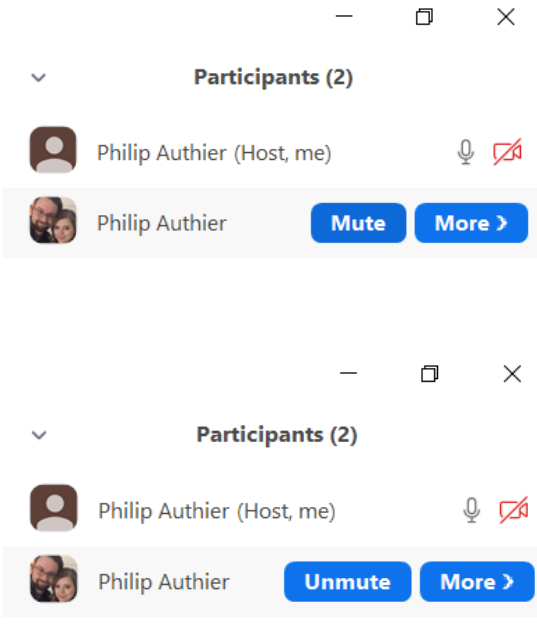
In the Settings Menu:

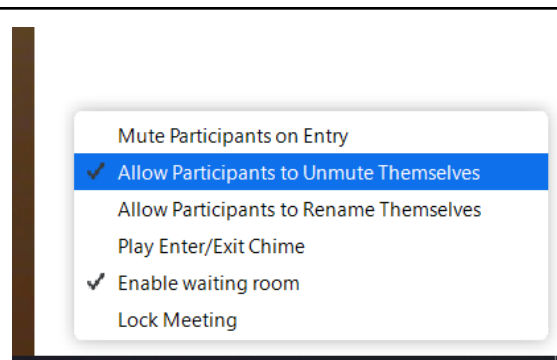
- 1. To set as default for all future scheduled meetings: find “Mute



How this feature increases security and management:

With large groups of participants or with groups of students, it can be helpful to have everyone muted upon entry. This minimizes chaotic background noise a session begins.

participants upon entry” and turn on. 2. When scheduling individual meetings you will have the option to turn this feature on or off.	 The screenshot shows the 'Meeting Options' panel. The option 'Mute participants upon entry' is checked and circled in red. Other options include 'Enable join before host', 'Enable waiting room', 'Breakout Room pre-assign', and 'Record the meeting automatically on the local computer'.	The host can mute and unmute participants and the participants can also mute and unmute themselves throughout the entirety of the session.
Hosts Can MUTE and UNMUTE Participants (On Session Dashboard) Hosts can also keep participants from unmuting themselves.	 The top screenshot shows the 'Participants (2)' list with 'Philip Authier (Host, me)' and 'Philip Authier'. The 'Philip Authier' entry has a 'Mute' button and a 'More >' button. The bottom screenshot shows the same list, but the 'Philip Authier' entry now has an 'Unmute' button instead of 'Mute'.	How this feature increases security and management: There may be instances when a participant is purposefully distracting, accidentally distracting or is unaware of the extent to which others can hear background noise in his/her location. In those cases, a host can easily use the mute function to mute individuals and minimize disruptions. The muted participant can unmute themselves to contribute.

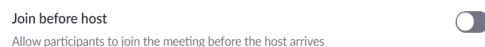


Using Settings and Features for Managing Participant Interactions

When Zooming with large groups of participants or with students, it can sometimes be difficult to manage. Zoom has several settings and features that can be used to help facilitate Zoom sessions.

Join Before Host Feature (In Settings)

1. This feature is turned **off** by default.
2. Only enable this feature if you are conferencing with ADULTS and are comfortable with the participants meeting before the host joins.



How this feature increases security and management:

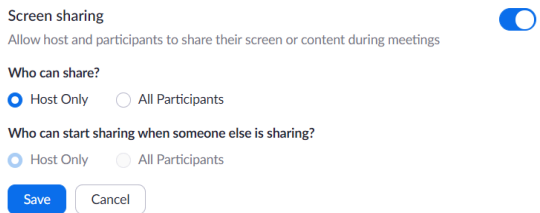
Keeping this feature set to OFF when creating a session prevents participants from entering a Zoom meeting and having audio and video access to other participants prior to the host entering the meeting.

If conferencing with students, always leave this feature set to OFF.

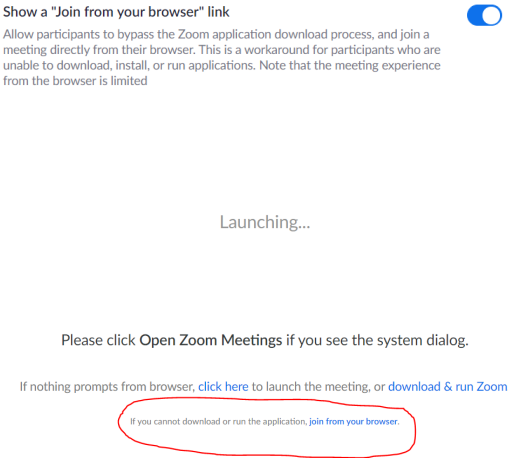
There may be instances with adult sessions where a host might set the 'Join Before Host' feature to ON so that participants may arrive early and engage

		in discussions.
Chat Feature (In Settings) 1. The Chat feature is ON by default. 2. This feature allows participants to text message each other during the meeting. The host CAN see these messages. 3. If desired, disable this feature by setting the toggle switch to the OFF position. 4. Note: If a participant is having difficulty with the audio on his/her devices, an enabled chat feature allows the host to communicate with the participant. 5. *NOTE - This can be turned OFF or ON during a live session by clicking the Security Shield icon.	Chat Allow meeting participants to send a message visible to all participants ☐ Prevent participants from saving chat ⓘ 	How this feature increases security and management: This chat feature can be very powerful when used appropriately and is most often left on for sessions with known adult participants. Disabling the Chat feature can keep participants from having inappropriate text discussions while in the Zoom session. Although the host can see these messages, it may take some time for the host to become aware and address the situation. Turning this feature off can provide additional security if you are working with unknown participants or with students by eliminating unwanted or inappropriate participant/participant and participant/whole group chat messages.
Private Chat Feature (In Settings) 1. Private Chat is ON by default. 2. Private Chat allows text messages between participants that the host does NOT see. 3. Turn private chat off, if private messages are a concern, by moving the toggle to the OFF position.	Private chat Allow meeting participants to send a private 1:1 message to another participant. 	How this feature increases security and management: This private chat feature can be very powerful when used appropriately and is most often left on for sessions with known adult participants. Disabling the Private Chat feature can

4. If working with students, it is safest to have this feature turned OFF. That eliminates inappropriate texting of which the host is unaware.		keep participants from having inappropriate text discussions while in the Zoom session that are NOT immediately visible to the host. Turning this feature OFF can provide additional security if you are working with unknown participants or with students by eliminating unwanted or inappropriate participant/participant chat messages of which the host is NOT aware.
File Transfer Feature (In Settings) 1. File Transfer is ON by default. 2. File transfer can be turned off, if desired. 3. Turning off File transfer can eliminate the transfer of unwanted or inappropriate files to participants. 4. If unwanted or unexpected file transfer is a concern, there are other options to transfer files between hosts and known participants. Ex. email, Google Classroom attachments, etc. If you have any questions on how to do this you may contact your Technology Integration Coach.	File transfer Hosts and participants can send files through the in-meeting chat.  	How this feature increases security and management: There are situations where a host wants participants to share files and it is appropriate to do so. Zoom.us has experienced issues where known and unknown users in a session share inappropriate files with other participants. If choosing to leave this feature enabled, consider using other safety features that will eliminate unknown/unwanted participants from joining your sessions thus minimizing the likelihood of unwanted sharing. Turning OFF this feature can eliminate unwanted or unexpected transfer of files from one participant to all participants in a group.

Screen Sharing Feature (In Settings) 1. Screen Sharing is set to All Participants by default. 2. Screen Sharing can be set to Host Only. 3. Make sure to click Save when the change has been made. 4. *NOTE - This can be turned OFF or ON during a live session by clicking the Security Shield icon.	 The screenshot shows the 'Screen sharing' settings in Zoom. At the top, there is a toggle switch that is turned on (blue). Below it, the text reads 'Allow host and participants to share their screen or content during meetings'. Under the heading 'Who can share?', there are two radio button options: 'Host Only' (which is selected) and 'All Participants'. Below this, under the heading 'Who can start sharing when someone else is sharing?', there are also two radio button options: 'Host Only' (selected) and 'All Participants'. At the bottom of the settings panel, there are two buttons: 'Save' (in blue) and 'Cancel' (in white with a grey border).	How this feature increases security and management: There are situations where a host wants participants to share screens and it is appropriate to do so. Zoom.us has experienced issues where known and unknown users in a session share screens unexpectedly during a session, often with offensive or inappropriate material. If choosing to leave this feature enabled, consider using other safety features that will eliminate unknown/unwanted participants from joining your sessions thus minimizing the likelihood of unwanted screen sharing. For sessions where it is not necessary for participants to share their screens, disabling this feature would increase security by eliminating unexpected or unwanted screen sharing by a participant.

Remote Control Feature (In Settings) 1. The Remote Control Feature is set to ON by default. 2. This allows the person who is sharing the screen to allow others to control the content.	Remote control During screen sharing, the person who is sharing can allow others to control the shared content 	How this feature increases security and management: This feature is on by default and rarely causes any issues. If you have concerns about accidentally giving someone else access to control the shared screen/content, then it may be best to disable this feature.
Virtual Background Feature (In Settings) 1. Virtual Background is ON by default. 2. This feature can be fun for participants and can provide a privacy option for those not wanting to show their surroundings during a video conference. 3. It is possible to turn this feature OFF, so that participants cannot add background images to their video. 4. Zoom has no way to block inappropriate images being set as a background if this feature is turned on.	Virtual background Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings. 	How this feature increases security: Zoom.us suggests disabling this feature in sessions with unknown participants. Zoom.us has no way to block inappropriate images from being added as a background. Note that participants can change backgrounds during a session. If this feature is enabled, the host should be prepared to stop video or remove a participant who enters with or changes to an offensive background. If choosing to leave this feature enabled, consider using other safety features that will eliminate unknown/unwanted participants from joining your sessions, thus minimizing the likelihood of inappropriate background images being

		visible to participants. When Zooming with students, some students may change backgrounds repeatedly during a session which can be distracting to that student and the other participants. When Zooming with students, you may want to set a group norm of only changing the background at the beginning of a session, or set this feature to OFF.
Join from your browser Feature (In Settings) 1. Turning this on will provide a link where participants can join a meeting without downloading an application to their computers. 2. Once enabled, using this feature requires a participant to click a different link than normal on the launch screen to enter a session. (See image)	 Show a "Join from your browser" link Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited Launching... Please click Open Zoom Meetings if you see the system dialog. If nothing prompts from browser, click here to launch the meeting, or download & run Zoom. If you cannot download or run the application, join from your browser.	How this feature increases security and management: When using Zoom with students, you may have situations where students are unable to download the Zoom app when joining a meeting. Enabling this feature allows access to the Zoom session without needing to download the app on their computers. The option to Join with your Browser, when enabled, shows on the launch screen and a participant would click the link at the bottom of that window to join a session. *NOTE that the meeting experience from the browser is limited.

BreakOut Room Feature - (In Settings) 1. Zoom offers Break Out Room options that allow a host to randomly or manually select small groups from within a live session. 2. Hosts can move participants in and out of breakout rooms and back to whole group. 3. Hosts can drop in and out of any or all breakout rooms.	Click here for Directions for BreakOut Rooms	How this feature increases security and management: Use of breakout rooms creates experiences for participants that are similar to common practices during in-person trainings. Use of this feature can be helpful to increase engagement and depth of interactions between participants.
Recording a Zoom Session - (In Settings) 1. There are situations where a host may want to record a Zoom to be available to watch at a later time. 2. It is best to set limits to only the host having the opportunity to record. This is particularly relevant when Zooming with students. 3. It is best practice to have participant permission to record a session. That ensures that all participants are aware before beginning that a session will be recorded.	Click here for Directions for Recording a Zoom session.	How this feature increases security and management: Use of the recording feature can be useful for sessions where someone might need to view the content at a later date. There are situations where this is useful and appropriate. Recognize, however, that there may be situations where recording may not be the best option. Be very thoughtful and purposeful when considering this option, particularly with students.

Using Dashboard Features in a Live Session to Increase Management

Zoom provides several features on the session dashboard that allows a host and participants to interact in ways

that mimic in person meetings or classes. Use of these features can help maximize engagement and minimize disruptions.

Annotate Over Content AND Whiteboard Feature (On Session Dashboard)

Zoom offers options during a live session for a host to annotate over content on a shared screen or display a blank whiteboard for drawing or writing.

[Click here for Directions for Annotating Over Content on a Shared Screen AND/OR Using the Whiteboard Feature](#)

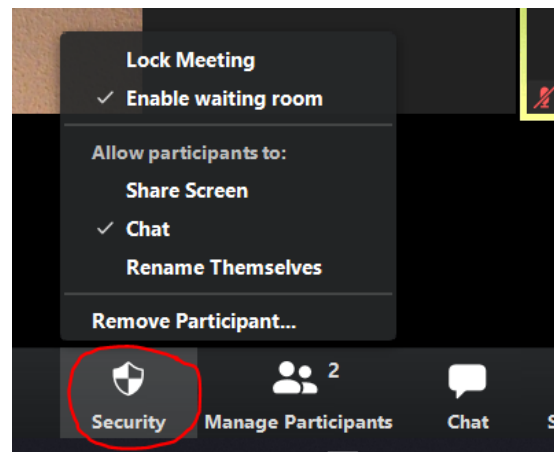
How this feature increases security and management:

Use of annotation over shared screen content or use of the whiteboard feature can increase engagement and clarity of information during a session.

Security Shield Icon (on Session Dashboard)

The Security Shield Icon on a live session dashboard allows the host to instantly engage and disengage several features that are generally set in settings when a session is created.

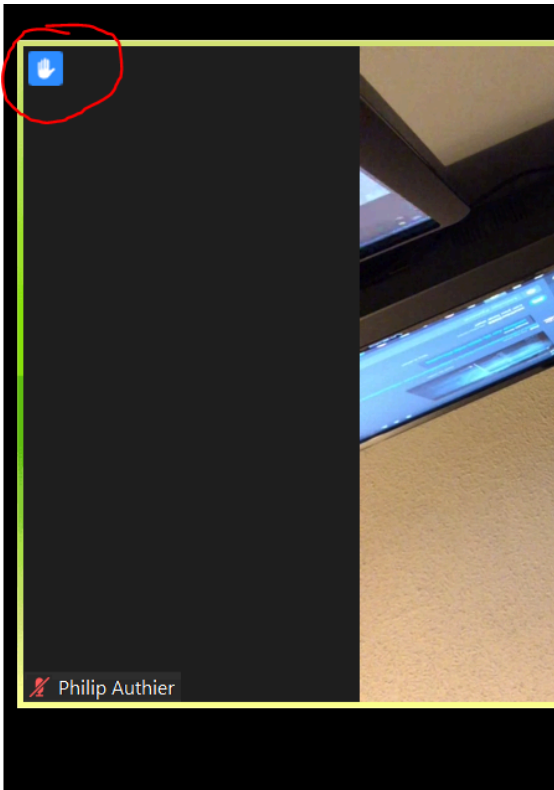
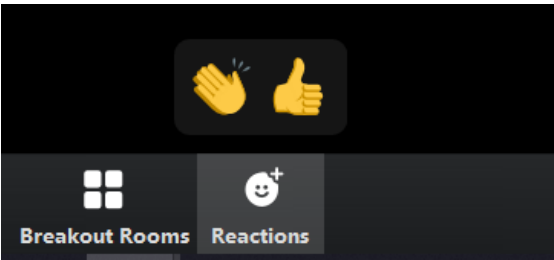
Hosts can click on the Security Shield Icon to engage or disengage settings for participants to share screens, chat, and rename themselves.



How this feature increases security and management:

The addition of the Security Shield Icon to the live session dashboard gives a host the ability to make changes to a Zoom session settings in real time.

Example: A host may have a session set to allow only the host to share a screen, but during the session a need arises for a participant to share a screen. Using the Shield Icon, the host can immediately change the setting to allow the participant to share.

Raise Hand Feature (On Session Dashboard)		How this feature increases security and management: This feature is helpful primarily as a management tool. It allows participants to signal to the host that they need help or wish to respond in much the same way as a face-to-face session. The host can see which participants have a 'raised hand' and respond accordingly.
Reactions Feature (On Session Dashboard)		How this feature increases security and management: This feature is helpful primarily as a management tool for increased engagement and feedback.

